ADBS_90913_Select AI - Phase 3 - Enhancement Bundle_TS

Author	SURYAPOGU AKSHAY RAJ
Epic	**ADBS-90913** - Select AI - Phase 3 - enhancement bundle IN PROGRESS
Test Specification Task	~~**ADBS-98753**~~ - Test Spec for Select AI - Phase 3 DONE
Functional and Design Specification Task	~~**ADBS-90915**~~ - Functional and Design Spec for Select AI - Phase 3 DONE
Status	FINAL

Available statuses:

- DRAFT - Author is initially working on the document
- REVIEW DRAFT - The document is ready for review
- REVISING - The document is under review
- FINAL - The document is complete and all reviews have been done

Reviewer	Reviewing	Reviewed with Comments	Approved
Tester1: SURYAPOGU AKSHAY RAJ Deepak Patel	☐	☐	☐
Dev1: Laura Zhao	☑	☑	☑
QA Manager: Varun Thakkar	☑	☑	☑
PM: Mark Hornick	☑	☑	☑

Bug Links

https://bug.oraclecorp.com/pls/bug/WEBBUG_REPORTS.Saved_Search?id=769141030425105425

Introduction

Overview of what is being tested

1. **Handle large schema by automatically detecting object list (23ai only):**
   Select AI will send metadata only for the specific tables relevant to the query rather than for all subscribed (tables covered by the provided AI profile) tables. This optimization leverages vector store capabilities to identify and send the most relevant table to reduce both the data payload and the cost of processing each prompt, and prevent exceeding LLM token limits. This feature is enabled using a new attribute object_list_mode = automated.
2. **Restrict SELECT AI SQL to use only objects listed in AI profile:**
   For chat agents or web users using SELECT AI over an application such as Apex, it is required that SELECT AI should generate SQL using only the tables listed in AI profile by the application developer. A new attribute enforce_object_list has been introduced to restrict SQL generation to only the tables specified in the AI profile's object list. When set to true, this attribute prevents accidental inclusion of system tables, dictionary views, or potential AI hallucinations involving LLM-generated table names. This attribute is not enabled by default.
3. **Use case insensitive comparison of column values for Select AI:**
   Select ai does not provide table data to LLM for SQL generation, so the exact case of specific column values is not known to LLM. Often, LLM produces a SQL WHERE clause by using exact case match of the values given the SELECT AI prompt. Executing the generated SQL may return no results from the database. A better approach is to use case insensitive comparison and provide matching results from database. A new attribute case_sensitive_values is provided for this feature and it is false by default.
4. **Disallow sending data to LLM:**
   Two new procedures enable_data_access and disable_data_access are introduced in the DBMS_CLOUD_AI package. These allow administrators to control whether Select AI can access and include actual schema table data in its SQL prompts. When data access is disabled, only metadata can be sent, and narrate/narrate for rag/generate_synthetic_data returns an error message, ensuring that sensitive data remains protected.

Test scenarios recommended by Development (to be filled by Development)

ⓘ **Suggested Tests**

Test Environments

- PDBCS VIEW/LABEL
- STABLE
- PRODUCTION

Test Case Design/Checklist

1. Handle large schema by automatically detecting object list (23ai only):

- **Enh 36870410 - SELECT AI : SEND ONLY SPECIFIC TABLES METADATA INSTEAD OF ALL SUBSCRIBED WITH EACH PROMPT**

object_list_mode parameter is introduced (values - all, automated)

Verify that for select AI query, only some tables metadata is used instead of all metadata using showprompt

- mention only the owner name in object_list and verify access to all tables
- mention only one table in object_list and verify prompt
- object_list empty with automated object_list_mode (expected - access to all objects)
- with invalid providers

Tests with the automatically created vector index:
After mentioning object_list_mode = automated|all, (compare the below test cases with both values)
To test for the variations of object_list mentioned in next section (2) -

- verify the automatic creation of vector index
    - check the attributes created with user_cloud_vector_index_attributes
    - query the tables created in contrast when the object_list_mode is set to all
- modify the attributes of the index with update_vector_index - attribute list
- modify the parameters of the pipeline with set_attribute - list of parameters
    - vary the object_list_mode as well from all automated and vice versa and verify with showprompt
- use set_attribute after update_vector_index (context - bug 37696743)
- create a vector index prior to usage of "automated" option with the same name convention to get index name already exists error or similar - <profile_name>_OBJECT_LIST_VECINDEX
- stop, run, run_only_once, start pipeline that is created with vector_index
- check automatic refresh - add tables|columns to vector index, delete tables|columns from vector index
- parameter object_list_mode tests (value = empty, null, invalid)

End-to-end and feature combination testing -

End to end test case

```
-- with object_list
SQL> BEGIN
  DBMS_CLOUD_AI.create_profile(
    'OCI_AUTO_TEST',
    '{"provider": "oci",
      "credential_name": "GENAI_CRED",
      "oci_compartment_id": "ocid1.compartment.oc1..
aaaaaaaar3sd2asx3l3ljkjyk34dxblvbmsaeflkrhndl2eswv7db4k5qjfa",
      "object_list": [{"owner": "OPTTEST5"}],
      "model" : "meta.llama-3.1-70b-instruct",
      "object_list_mode": "automated"
      }');
END;

PL/SQL procedure successfully completed.

SQL> EXEC DBMS_CLOUD_AI.set_profile('OCI_AUTO_TEST');

PL/SQL procedure successfully completed.

SQL> select ai showsql Find the number of audits that require a follow-up;
 -- verify the tables used are the ones mentioned in object_list, use showprompt for the same
```

2. Restrict SELECT AI SQL to only use objects listed in AI profile:

- **Enh 36821878 - PROVIDE OPTION TO RESTRICT TABLES USED TO THOSE LISTED IN AI PROFILE OBJECT LIST**

Introduced parameter enforce_object_list (values - true, false)

- Verify that other tables access is restricted with select AI queries when enforce_object_list is TRUE using showprompt and showsql with query
- set enforce_object_list as TRUE verify with showsql the access is only for tables specified in object_list
- Update the object_list and verify that it is enforced with showprompt, showsql

Cases for object_list -

- Owner/entire schema
- few tables in schema
- few tables in one schema and few tables from different schema
- No mention of object_list
- NULL
- empty
- invalid (tables)

3. Use case insensitive comparison of column values for Select AI:

- **Enh 36628115 - ADDRESS CASE SENSITIVITY IN COLUMN VALUES FOR SELECT AI**

Use existing select AI prompts with case sensitive prompts

- set case_sensitive_values to false verify query (showsql) has insensitive verify in showprompt about case sensitivity (what prompt says about this)
- use double quotes with case_sensitive_values as false verify query with sensitive case
- set case_sensitive_values to true verify query with sensitive case

4. Disallow sending data to LLM:

- **Enh 36870169 - ADD PROCEDURE TO ENABLE/DISABLE AUGMENTING SELECT AI PROMPT WITH SCHEMA TABLE DATA**

Tests for the procedures -

- Check data flow for narrate action for both RAG and SQL Generation
- Check data flow for Synthetic Data Generation
- Check data flow for GENERATE API

Other test cases (combinatorial, different use cases etc) -

1. query information that would use more than the match_limit number of tables (default 10) with object_list_mode (automated|all)
2. test the combination of object_list_mode (all|automated) and enforce_object_list (TRUE|FALSE)

Security Vulnerability

(includes tests for all four sections(enhancements) above)

- Disable dataflow via ADMIN and verify the features RAG, SDG - should return error - check modification via user
- Enable dataflow via ADMIN and verify the working of features RAG, SDG
- Enable/Disable of dataflow by user - should return error since user doesnt have access
- enforce_object_list set to TRUE and verify access to unspecified tables in object_list with showsql
- User without access to DBMS_CLOUD_AI cannot modify the parametrs
- Override the prompt to skip enforcing the object list

Database Releases

- 19c (negative tests)
- 23ai

Database Types

NA

Service Types

NA

Test Categories

LRG Tests

Service Deployment Layer

NA

Provisioning Layer/LCM

NA

Monitoring Layer

NA

Data Sources Layer

NA

Database Layer

NA

Security Layer/Products

NA

Mongo API integration

NA

User Application Layer/Products

NA

Voluntary Product Accessibility Template (VPAT)

NA

Service Patching & Upgrade

NA

Concurrency Testing

NA

BUT(Broker Unit Testing)

NA

Bug Filing Convention

Add the tag of epic - ADBS_90913

Point of Contacts

QA - SURYAPOGU AKSHAY RAJ
Deepak Patel

PDBCS Label

NA

Details of How to Start Testing this Epic

NA

References

ADBS_90913_Select AI - Phase 3 - Enhancement Bundle_FDS